Qualys File Integrity Monitoring (FIM)

Release Notes

Version 3.6

December 06, 2022

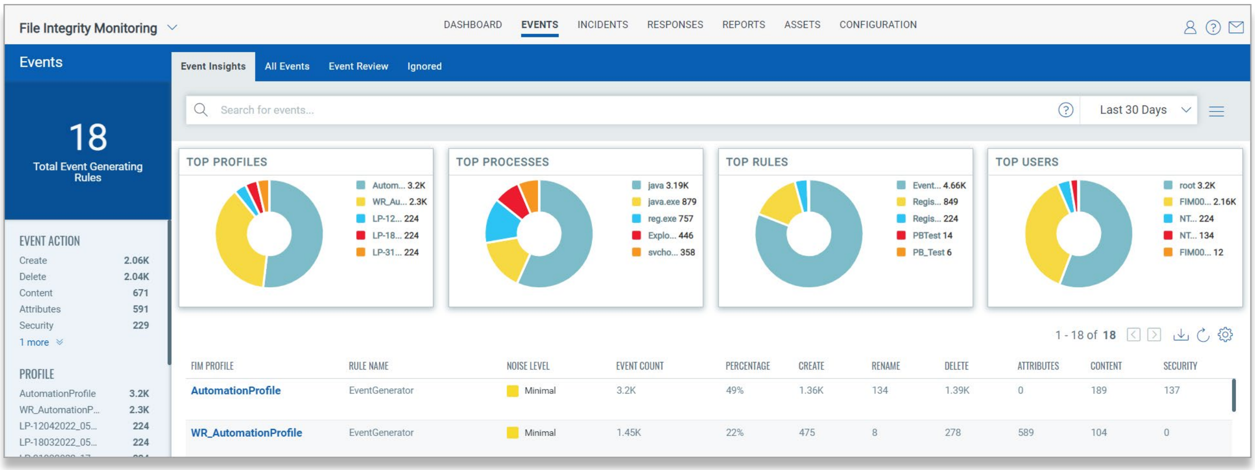
Here's what's new in Qualys File Integrity Monitoring 3.6!

New Features

Event Insights Tab for Efficient Fine-Tuning of Events

This release introduces the new **Event Insights** sub-tab under the **Events** tab, which helps you have a thorough insight into the change events on your FIM console. The **Event Insights** tab includes a list of the FIM profiles that have generated the highest number of events. It also contains widgets with event data, which can be drilled down to access granular data.

The widgets in the **Event Insights** tab display specific data generated within the time frame that's selected from the time range selector. The widgets help you with a single-glance perception of the top event generators; thereby enabling you to analyze your rules and pinpoint which rule in which profile has generated the maximum number of events.



EVENT ACTION	
Create	2.06K
Delete	2.04K
Content	671
Attributes	591
Security	229

PROFILE	
AutomationProfile	3.2K
WR_AutomationP...	2.3K
LP-12042022_05...	224
LP-18032022_05...	224

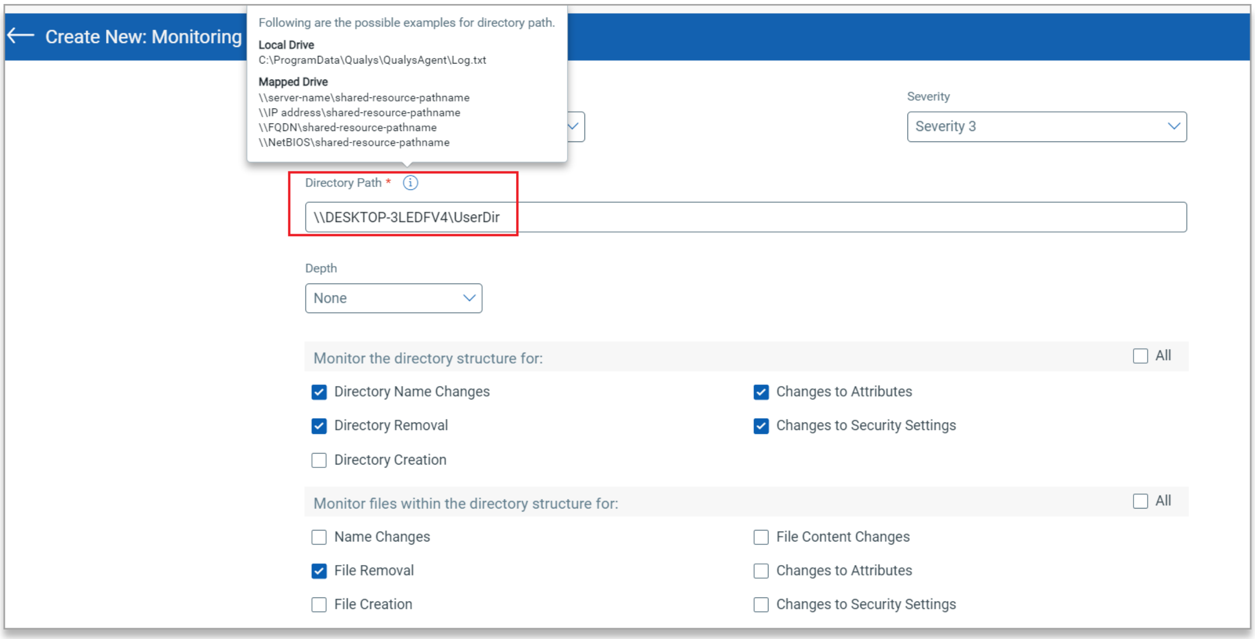
FIM PROFILE	RULE NAME	NOISE LEVEL	EVENT COUNT	PERCENTAGE	CREATE	RENAME	DELETE	ATTRIBUTES	CONTENT	SECURITY
AutomationProfile	EventGenerator	Minimal	3.2K	49%	1.36K	134	1.39K	0	189	137
WR_AutomationProfile	EventGenerator	Minimal	1.45K	22%	475	8	278	589	104	0

The event noise level is displayed as 'Minimal', 'Moderate' and 'Critical', where, 'Critical' indicates that the corresponding rule is generating more than 90% of the events. You can select a profile and fine-tune the rule to ensure reduced event noise.

Monitor Mapped Network Drive on Windows Hosts

This release adds the capability to monitor files and directories on mapped network drives. With this new feature, you can expand your monitoring scope to include change events that are not just limited to physical drives on the host, but expands to logical drives as well. While creating a FIM profile rule, you can add the Universal Naming Convention (UNC) path as the base directory in the **Directory Path** text box available on the **Rule Details** page. Use any of the following formats to specify the directory or file name to be monitored:

- \\server-name\shared-resource-pathname
- \\IP address\shared-resource-pathname
- \\FQDN\shared-resource-pathname
- \\NetBIOS\shared-resource-pathname



Following are the possible examples for directory path.

Local Drive
C:\ProgramData\Qualys\QualysAgent\Log.txt

Mapped Drive
\\server-name\shared-resource-pathname
\\IP address\shared-resource-pathname
\\FQDN\shared-resource-pathname
\\NetBIOS\shared-resource-pathname

Severity: Severity 3

Directory Path *: \\DESKTOP-3LEDFV4\UserDir

Depth: None

Monitor the directory structure for: □ All

☑ Directory Name Changes
☑ Directory Removal
□ Directory Creation
☑ Changes to Attributes
☑ Changes to Security Settings

Monitor files within the directory structure for: □ All

□ Name Changes
☑ File Removal
□ File Creation
□ File Content Changes
□ Changes to Attributes
□ Changes to Security Settings

The support added for mapped network drives to be monitored ensures that you do not have any blind spots left in your efforts towards preventing potential unauthorized access in your file systems.

Enhanced Role-Based Access Control for FIM User Accounts

With this release, Qualys FIM has implemented enhanced role-based access control for all user accounts. Now, FIM user accounts have access only to the specific tasks that they have permission for. This ensures that users can perform relevant actions depending on the roles and permissions that have been assigned. A Manager user can use the Qualys Administration module to create FIM users and assign roles and permissions.

With this new enhancement, Qualys FIM adds an additional layer of security to accomplish required tasks within your organization and prevent unauthorized users from accessing anything that's beyond their assigned roles.

For more information on the predefined roles and the associated permissions, refer to the Roles and Permissions in FIM topic in Qualys FIM Online Help.

New User Roles for Efficient Role-Based Operations

Qualys FIM has introduced new user roles to ensure efficient management of role-based operations.

A user with the Manager role is the super-user and has all the FIM permissions by default. The Manager user can create other users and assign roles.

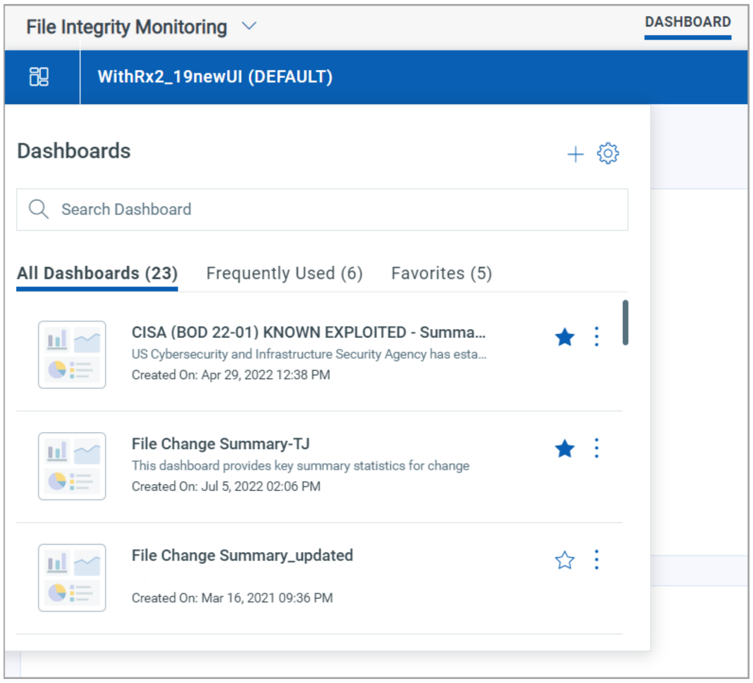
The following table includes information on the user roles and their respective rights and privileges:

Role	Permissions
FIM Manager	• **General UI:** Access • **Dashboard:** Create, Update, Delete, Print

Role	Permissions
	• **Events:** View, Ignore, Whitelist, Event Insights, Download • **Incidents:** View, Create, Update, Review, Reopen, Download • **Correlation Rules:** View, Create, Update, Delete, Activate, Deactivate • **Reports:** View, Create, Delete, Download • **Report Rules:** View, Create, Update, Delete, Schedule, Resume, Pause • **Profiles:** View, Create, Update, Delete, Activate, Deactivate, Link, Assign, Download • **Profile Library:** View, Import, Download • **Asset:** View, Download • **Responses (alerting):** Access, Create, Edit, Delete • **Responses (alerting rules):** Create, Edit, Delete
FIM Author	• **General UI:** Access • **Dashboard:** Create, Update, Print • **Events:** View, Event Insights, Download • **Incidents:** View, Create, Update, Download • **Correlation Rules:** View, Create, Update • **Reports:** View, Create, Download • **Report Rules:** View, Create, Download • **Profile:** View, Create, Update, Download, Link, Assign • **Profile Library:** View, Import, Download • **Assets:** View, Download • **Responses (alerting):** Access Alert, Create Alert, Edit Alert • **Responses (alerting rules):** Create, Edit
FIM Auditor	• **General UI:** Access • **Dashboard:** Print • **Events:** View, Download • **Incidents:** View, Download • **Correlation Rules:** View • **Reports:** View, Download • **Report Rules:** View • **Profiles:** View, Download • **Profile Library:** View, Download • **Assets:** View, Download • **Responses (alerting):** Access Alert
FIM Analyst	• **General UI:** Access • **Dashboard:** Create, Update, Print • **Events:** View, Ignore, Whitelist, Event Insights, Download • **Incidents:** View, Create, Update, Review, Reopen, Download • **Correlation Rules:** View, Create, Update, Activate, Deactivate • **Reports:** View, Create, Download • **Report Rules:** View, Create, Update, Schedule, Resume, Pause • **Profiles:** View, Create, Update, Activate, Deactivate, Link, Assign, Download • **Profile Library:** View, Import, Download • **Assets:** View, Download • **Responses (alerting):** Access Alert, Create Alert, Edit Alert • **Responses (alerting rules):** Create, Edit

New Dashboard Layout for Easy Access to the Dashboard Functions

You can now edit a dashboard or change the layout of the widgets in the dashboard. Click ⊞ to open the **Dashboards** panel.



CISA (BOD 22-01) KNOWN EXPLOITED - Summa...
US Cybersecurity and Infrastructure Security Agency has esta...
Created On: Apr 29, 2022 12:38 PM

File Change Summary-TJ
This dashboard provides key summary statistics for change
Created On: Jul 5, 2022 02:06 PM

File Change Summary_updated
Created On: Mar 16, 2021 09:36 PM

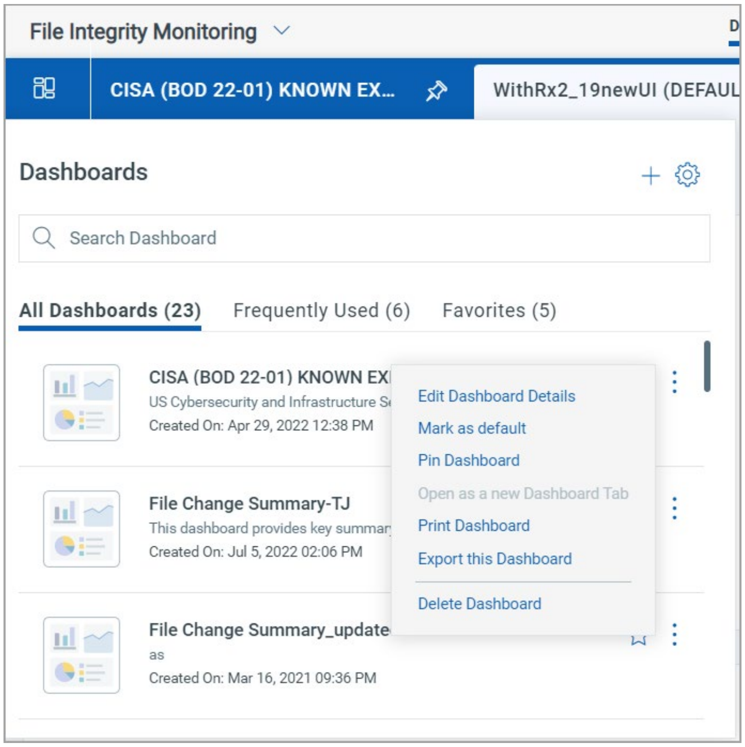
The **Dashboards** panel contains three tabs to let you do the following:

- View all the current dashboards
- View the frequently used dashboards
- View the favorite dashboards

You can click + to go to the **Add or Customize Dashboard templates** page. You can also click ⚙ to go to the **Manage Dashboards** page.

Select a dashboard and click ⋮ to perform any of the following actions:

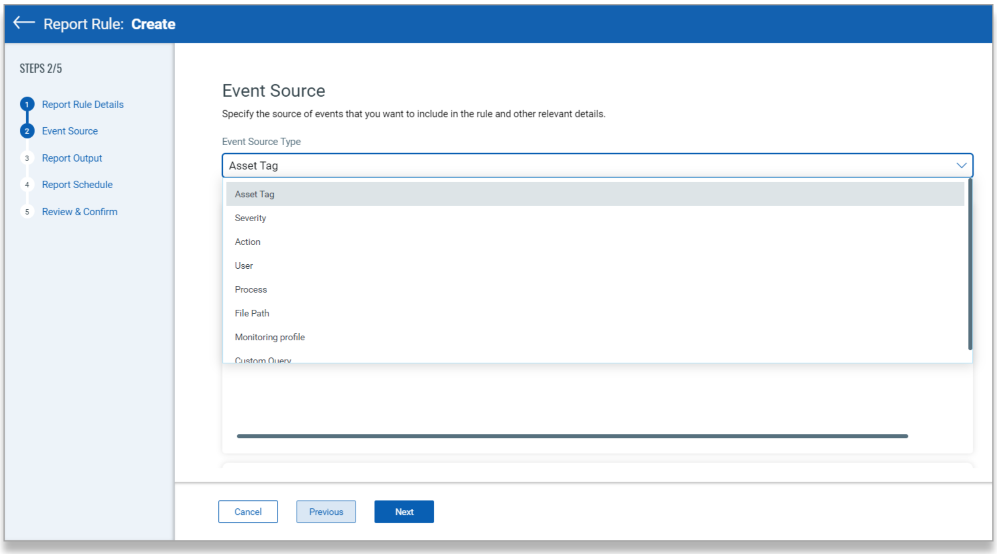
- Edit the dashboard details.
- Mark the selected dashboard as the default dashboard.
- Pin the dashboard. The pinned dashboard is displayed on the dashboard panel even after you log out from your account or refresh the page.
- Open the selected dashboard as a new dashboard tab on the dashboard panel.
- Print the dashboard that you have selected.
- Export the selected dashboard.
- Delete the selected dashboard.


File Integrity Monitoring
CISA (BOD 22-01) KNOWN EX...
WithRx2_19newUI (DEFAUL
Dashboards
Search Dashboard
All Dashboards (23)
Frequently Used (6)
Favorites (5)
CISA (BOD 22-01) KNOWN EX
US Cybersecurity and Infrastructure S
Created On: Apr 29, 2022 12:38 PM
File Change Summary-TJ
This dashboard provides key summar
Created On: Jul 5, 2022 02:06 PM
File Change Summary_update
as
Created On: Mar 16, 2021 09:36 PM
Edit Dashboard Details
Mark as default
Pin Dashboard
Open as a new Dashboard Tab
Print Dashboard
Export this Dashboard
Delete Dashboard

Enhanced Reporting

Previously in the report rule creation process, only custom queries were supported to specify event sources. This release adds several event sources that can just be selected from the drop-down list:

- Asset Tag
- Severity
- Action
- User
- Process
- File Path
- Monitoring Profile



Event Source

Specify the source of events that you want to include in the rule and other relevant details.

Event Source Type: Asset Tag

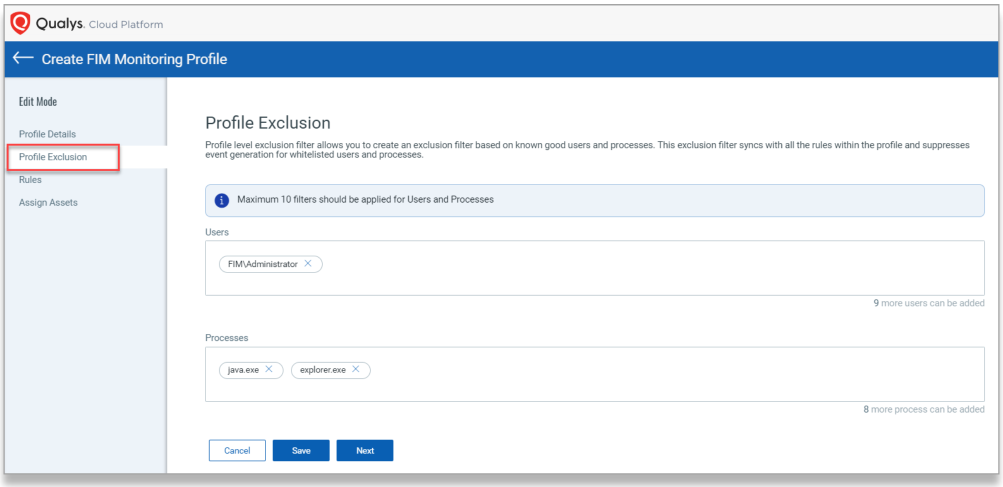
Introduction of User-Based and Process-Based Inclusion-Exclusion Filters

You can add user-based and process-based inclusions and exclusions to reduce event noise. In simple terms, known good users or processes can be excluded so that such events are dropped at the agent level, and false positives do not reach the Qualys platform. Alternatively, suspicious users or processes can be included to ensure that events generated by specific users or processes are never missed for defined monitored locations.

User-based and process-based inclusions or exclusions can be added at the rule level in the FIM profile.

Besides, you can also specify the profile-level exclusion filters, which act as global exclusion filters for a specific FIM profile. If you add a profile-level exclusion filter, it gets inherited by each rule under that profile.

Note: User-based and process-based filtering is currently available on Windows platform only.



Profile Exclusion

Profile level exclusion filter allows you to create an exclusion filter based on known good users and processes. This exclusion filter syncs with all the rules within the profile and suppresses event generation for whitelisted users and processes.

Maximum 10 filters should be applied for Users and Processes

Users: FIM\Administrator

9 more users can be added

Processes: java.exe, explorer.exe

8 more process can be added

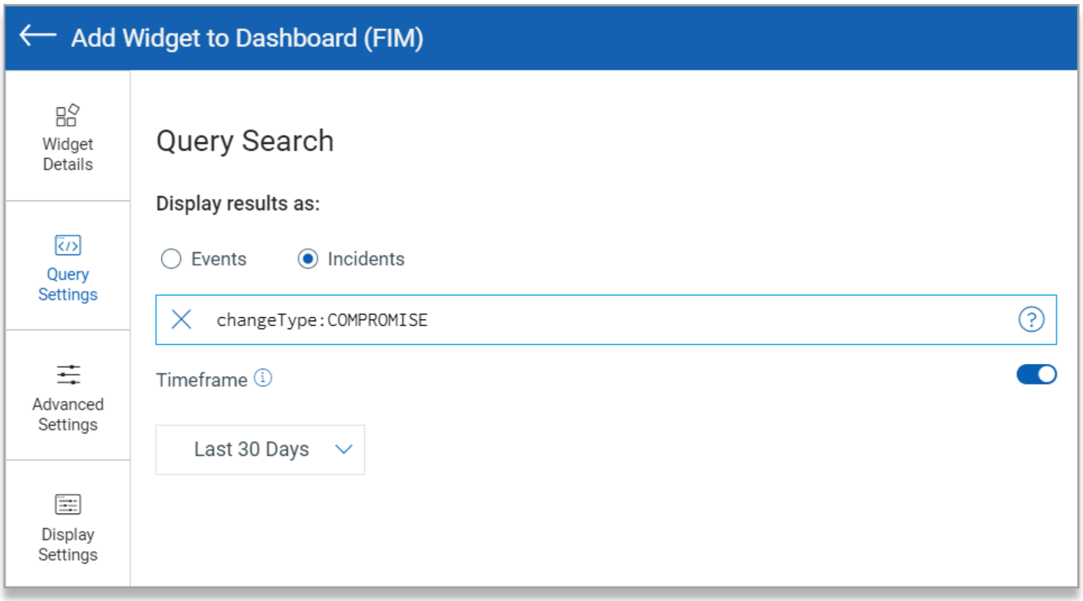
Option to Include Incidents While Creating a Dashboard Widget

You can now select the option to create a widget for FIM incidents as well. In the **Query Settings** page of the Widget Builder, select **Incidents** and do the following:

Enter the QQL token to specify the type of incident and select one of the following change event types:

- Automated
- Compromise
- Manual
- Other

Optionally, select the time range for the incidents generated.



Display results as:

○ Events ● Incidents

```
changeType:COMPROMISE
```

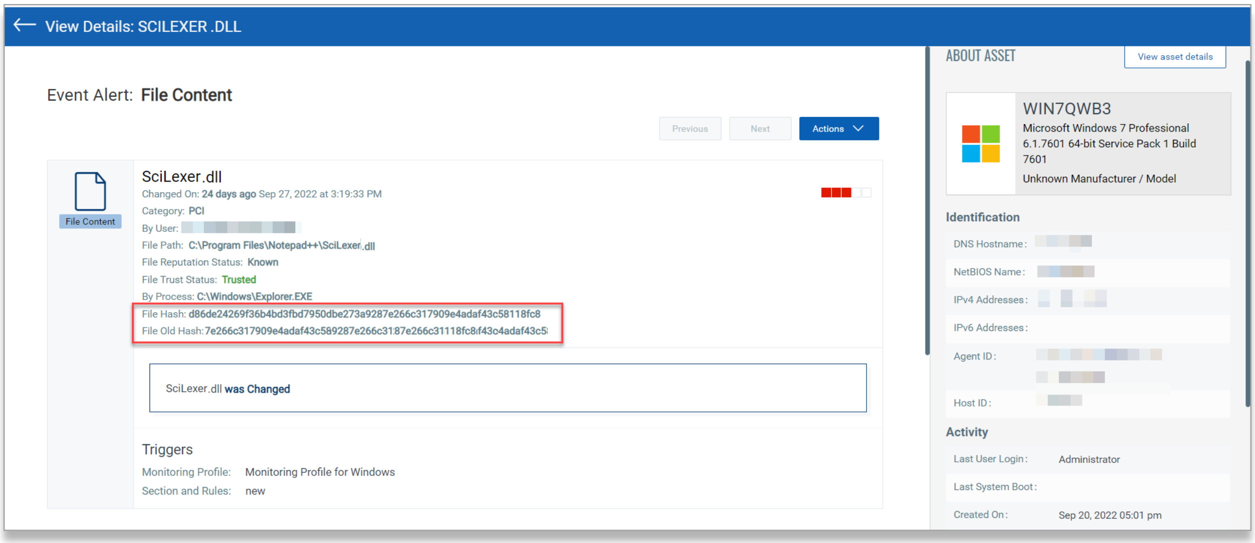
Timeframe: on

Last 30 Days

The newly created widget includes data for FIM incidents as per your specifications.

Introduction of Old and New Hash Values for Content Change Events

Earlier, the **Event Details** page for file changes used to display only the current file hash value. Starting this release, Qualys FIM captures the old hash as well as the new hash values.



View Details: SCILEXER .DLL

Event Alert: **File Content**

SciLexer.dll

Changed On: **24 days ago** Sep 27, 2022 at 3:19:33 PM

Category: **PCI**

By User: [redacted]

File Path: **C:\Program Files\Notepad++\SciLexer.dll**

File Reputation Status: **Known**

File Trust Status: **Trusted**

By Process: **C:\Windows\Explorer.EXE**

File Hash: **d86de24269f36b4bd3fbd7950dbe273a9287e266c317909e4adaf43c58118fc8**

File Old Hash: **7e266c317909e4adaf43c589287e266c3187e266c31118fc8f43c4adaf43c5**

SciLexer.dll **was Changed**

Triggers

Monitoring Profile: Monitoring Profile for Windows

Section and Rules: new

ABOUT ASSET

WIN7QWB3

Microsoft Windows 7 Professional 6.1.7601 64-bit Service Pack 1 Build 7601

Unknown Manufacturer / Model

Identification

DNS Hostname: [redacted]

NetBIOS Name: [redacted]

IPv4 Addresses: [redacted]

IPv6 Addresses:

Agent ID: [redacted]

Host ID: [redacted]

Activity

Last User Login: Administrator

Last System Boot:

Created On: Sep 20, 2022 05:01 pm

Enhanced Limit on Inclusion and Exclusion Filters and File Paths

The limit of inclusion and exclusion filters that can be applied to directories and files has been increased to a maximum of 15 filters. For each filter, user can add up to 20 file paths.

Fixed Issues

- Earlier, while creating a configuration profile, an error message used to be displayed when users entered a numerical value in the **Create New Category** > **Category Name** field in the **Profile Details** and **Section Details** pages. This issue is fixed, and alphanumeric characters are now accepted in the **Category Name** text box.

- The incident report did not contain the hostnames of the FIM assets. This is now fixed, and the hostname is now displayed in the reports.

- Details about attribute changes were not captured on the **Event Details** page. Because of this, event details did not contain information relevant to the attribute changes in a file. This release fixes this issue, and now attribute changes are correctly captured on the **Event Details** page.

Known Issue

If a user renames an existing incident and re-generates the incident report, the previous records of the incident report also get renamed.